配置安全電子郵件網關出站MTA-STS

目錄

簡介

本文描述配置安全電子郵件網關(SEG)出站郵件傳輸代理 — 嚴格傳輸安全(MTA-STS)的步驟。

必要條件

需求

思科安全電子郵件網關(SEG)常規設定和配置的一般知識。

採用元件

此安裝程式需要：

- Cisco Secure Email Gateway(SEG)AsyncOS 16.0或更高版本。
- 目標控制配置檔案。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

概觀

Mail Transfer Agent - Strict Transport Security(MTA-STS)是一種協定，強制使用帶有附加安全保護層的安全TLS連線。MTA-STS通過確保通過安全、加密的管道傳送電子郵件，幫助防止中間人攻擊和竊聽。

SEG AsyncOS 16和更新版本可以執行出站MTA-STS消息傳遞至已配置的MTA-STS接收域。

啟用後，SEG會檢查目標控制配置檔案的MTA-STS設定。SEG啟動MTA-STS進程以獲取、驗證和應用定義的記錄和策略，從而確保通過TLSv1.2或更高版本安全地連線到接收MTA。

接收域所有者負責建立、發佈和維護DNS記錄和MTA-STS策略。

MTA-STS如何在SEG中運行

- 接收域維護MTA-STS策略和MTA-STS DNS文本記錄。
- 傳送域MTA必須是能夠解析目標域MTA-STS策略並對其執行操作的MTA-STS。

Receiving Email Domain所有者通過DNS發佈MTA-STS txt記錄，如下所述：

- txt記錄會觸發SEG檢查MTA-STS策略，該策略託管在啟用HTTPS的Web伺服器上。
- 策略指定用於與域通訊的引數。
  - 包含要接收的MTA-STS MX主機。
  - 模式定義為測試模式或強制模式
  - 需要TLSv1.2或更高版本。

- MTA-STS使用DNS TXT記錄進行策略發現。它從HTTPS主機獲取MTA-STS策略。
- 在TLS握手期間，HTTPS伺服器必須提供「MTA-STS」DNS-ID的有效X.509證書。

Sending Email Domain 方面：

- 當SEG（傳送MTA）向MTA-STS域傳送電子郵件時，它會首先檢查收件人域MTA-STS策略。
- 如果策略配置為強制模式，則傳送電子郵件伺服器會嘗試與接收電子郵件伺服器（接收MTA）建立安全、加密的連線。 如果無法建立安全連線（例如，如果TLS證書無效或連線降級為不安全的協定），則電子郵件將無法傳送，並將失敗通知發件人。

RFC8461

設定

安裝過程中建議採取初步措施：

1.在配置SEG目標控制配置檔案之前，驗證目標域是否具有正確配置的MTA-STS DNS記錄和策略記錄。

- 這是通過訪問MTA-STS檢查器網頁執行的最有效的操作。
  - Google搜尋「驗證MTA-STS域」
  - 從搜尋結果中選擇驗證網站。
  - 輸入目標域。
- 僅在驗證檢查完成之後配置域。

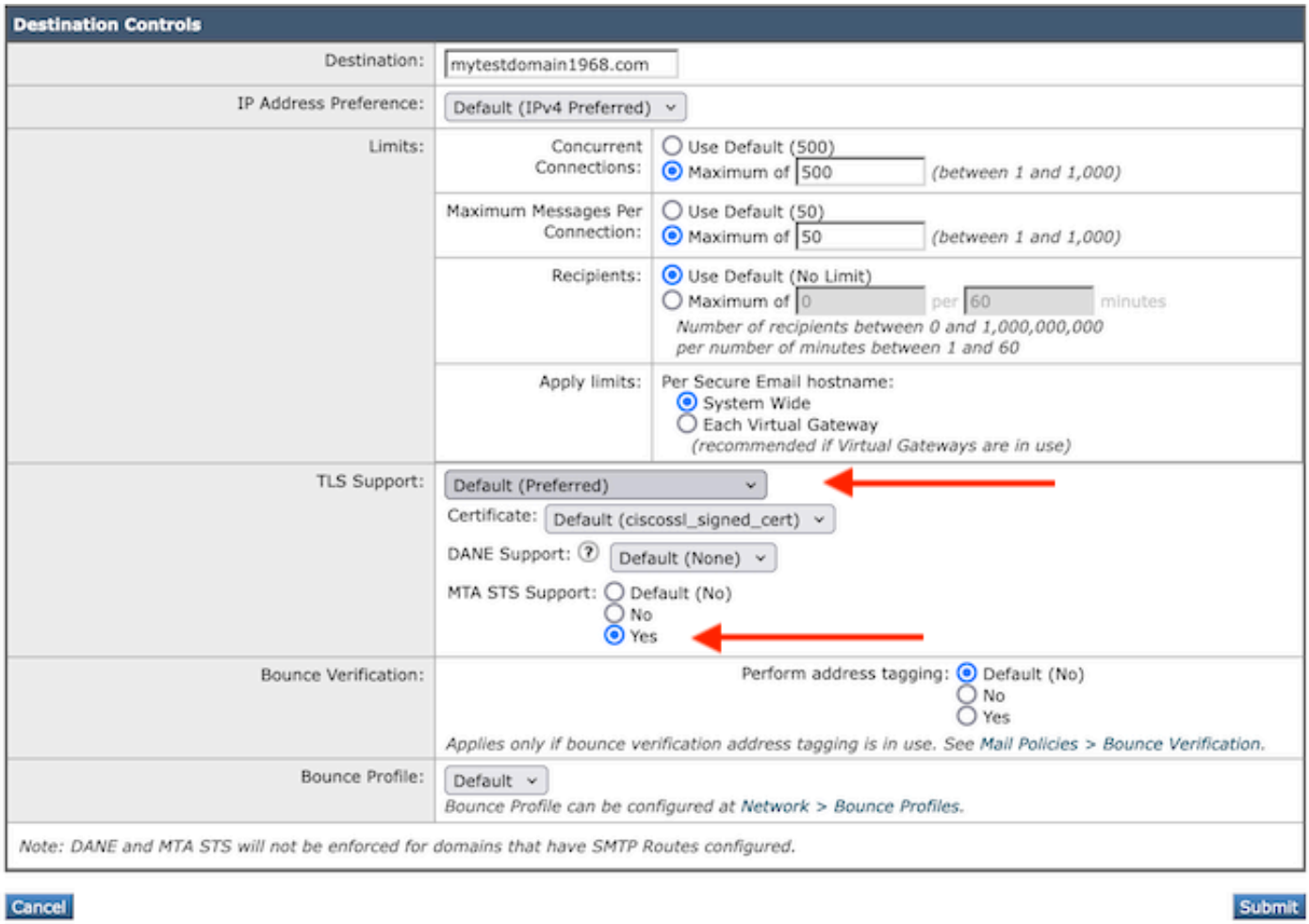
2. 不要在目的地控制預設原則上使用MTA-STS。

- 配置為利用MTA-STS的每個目標控制配置檔案會為SEG增加較小的負擔。如果預設目標控制策略配置了MTA-STS，而不驗證域，則可能會影響SEG服務。

WebUI配置

- 導航到郵件策略>目標控制頁。
- 選擇Add Destination Controls或編輯現有目標控制配置檔案。
  - TLS支援設定允許除無之外的任何設定，其中含有各種TLS支援選項。
  - 子選單DANE Support Options包括Mandatory、Opportational或None。
  - MTA-STS支援設定=是
- 選擇提交，然後選擇提交以應用更改。

附註：如果接收MTA駐留在Gsuite或O365等託管環境中，請將目標控制TLS配置為TLS Required-Verify託管域。



目標控制配置檔案

互通性注意事項：

DANE支援優先於MTA STS，並可能影響所採取的操作：

- 如果DANE成功，則會跳過MTA-STS並傳送郵件。
- 如果DANE強制失敗，則不會傳送郵件。
- 如果DANE Opportunity失敗，並且由於配置錯誤而跳過MTA-STS，則SEG會嘗試使用配置的TLS設定進行傳送。
- 如果為域配置了SMTP路由，則不應用MTA-STS。

CLI組態

- destconfig
  - 新建/編輯
    - 輸入首選選項，直到顯示TLS選項選單項。
    - TLS選項2-6支援MTA-STS。

是否要為此域應用特定TLS設定？[N]> y

是否要使用TLS支援？
1.否
2.首選
3.必填
4.首選 — 驗證
5.必需 — 驗證
6.必需 — 驗證託管域
[2]>2

您已選擇啟用TLS。請使用certconfig命令確保配置了有效的證書。
是否要配置DANE支援？[N]>

是否要配置MTA STS支援？[N]> y

是否要使用MTA STS支援？
1.關閉
2.在
[1]> 2

未對已配置SMTP路由的域實施MTA STS:

1. 完成剩餘選項以完成特定目標控制配置檔案。
2. 使用Submit > Commit應用更改。

驗證

資訊級別mail_logs:

```
Thu Sep 26 15:23:39 2024 Info: Successfully fetched MTA-STS TXT record for domain(mta-test.domain.com)
Thu Sep 26 15:23:40 2024 Info: New SMTP DCID 834833 interface 10.1.1.2 address 10.1.1.3 port 25
Thu Sep 26 15:23:41 2024 Info: DCID 834833 TLS success protocol TLSv1.3 cipher TLS_AES_256_GCM_SHA384 s
Thu Sep 26 15:23:41 2024 Info: MTA-STS policy for the domain (domain.com) Successful.
Thu Sep 26 15:23:41 2024 Info: Delivery start DCID 834833 MID 5444 to RID [0]
Thu Sep 26 15:23:44 2024 Info: Message finished MID 5444 done
```

debug level mail_logs:

```
Thu Sep 26 15:23:39 2024 Debug: DNS query: Q(_mta-sts.domain.com, 'TXT')
Thu Sep 26 15:23:39 2024 Debug: DNS query: QN(_mta-sts.domain.com, 'TXT', 'recursive_nameserver0.parent
Thu Sep 26 15:23:39 2024 Debug: DNS query: QIP (_mta-sts.domain.com,'TXT','10.10.5.61',15)
Thu Sep 26 15:23:39 2024 Debug: DNS encache (_mta-sts.domain.com, TXT, [(131794459543073830L, 0, 'insec
Thu Sep 26 15:23:39 2024 Info: Successfully fetched MTA-STS TXT record for domain(domain.com)
Thu Sep 26 15:23:39 2024 Debug: Valid cache entry found for the domain (domain.com).Thu Sep 26 15:23:39
Thu Sep 26 15:23:39 2024 Debug: DNS query: QIP (domain.com,'MX','10.10.5.61',15)
Thu Sep 26 15:23:39 2024 Info: Applying MTA-STS policy for the domain (domain.com)
Thu Sep 26 15:23:40 2024 Info: New SMTP DCID 834833 interface 10.1.1.2 address 10.1.1.3 port 25
Thu Sep 26 15:23:41 2024 Debug: DNS query: Q(domain.com, 'MX')
Thu Sep 26 15:23:41 2024 Info: DCID 834833 TLS success protocol TLSv1.3 cipher TLS_AES_256_GCM_SHA384 su
Thu Sep 26 15:23:41 2024 Info: MTA-STS policy for the domain (domain.com) Successful.
Thu Sep 26 15:23:41 2024 Info: Delivery start DCID 834833 MID 5444 to RID [0]
Thu Sep 26 15:23:44 2024 Info: Message finished MID 5444 done
```

接收SEG支援的TLS v1.3:

```
Wed Jan 17 21:09:12 2024 Info: ICID 1020089 TLS success protocol TLSv1.3 cipher TLS_AES_256_GCM_SHA384
```

2024年9月24日星期二09:13:52 2024年調試：DNS查詢：Q(_mta-sts.domain.com, 'TXT')
2024年9月24日星期二09:13:52 2024年調試：DNS查詢：QN(_mta-sts.domain.com, 'TXT', 'recursive_nameserver0.parent')
2024年9月24日星期二09:13:52 2024年調試：DNS查詢：QIP(_mta-sts.domain.com,'TXT','10.10.5.61',15)
2024年9月24日星期二09:13:52 2024年調試：DNS快取(_mta-sts.domain.com, TXT，[(13136652570158050 8L， 0, 'insecure',('v=STSv1;id=12345678598Z;',)])
2024年9月24日星期二09:13:52 2024資訊：已成功獲取域(domain.com)的MTA-STS TXT記錄
2024年9月24日星期二09:13:52 2024年調試：獲取域的MTA-STS策略(domain.com)
2024年9月24日星期二09:13:52 2024年調試：通過代理請求MTA-STS策略獲取
2024年9月24日星期二09:13:52 2024年調試：由於連線超時，請求獲取STS策略失敗。對於域domain.com
2024年9月24日星期二09:13:52 2024資訊：獲取域的MTA-STS策略時遇到故障(domain.com)

2024年9月19日週四13:04:50資訊：已成功獲取域(domain.com)的MTA-STS TXT記錄
2024年9月19日週四13:04:50調試：獲取域的MTA-STS策略(domain.com)
2024年9月19日週四13:04:50調試：通過代理請求MTA-STS策略獲取
2024年9月19日週四13:04:50調試：由於連線超時，請求獲取STS策略失敗。對於域domain.com
2024年9月19日週四13:04:50資訊：獲取域的MTA-STS策略時遇到故障(domain.com)

2024年9月19日週四13:04:50資訊：MID 5411排隊等待交付

疑難排解

1.如果SEG無法傳送，並出現「peer cert does not match domain.com」錯誤。

這表示目標為託管服務，如G Suite或M365。更改Destination Controls Profile TLS設定>需要TLS — 驗證託管域:

```
Tue Sep 24 10:02:52 2024 Info: DCID 831556 TLS deferring: verify error: peer cert does not match domain
Tue Sep 24 10:02:52 2024 Info: DCID 831556 TLS was required but could not be successfully negotiated
```

2.如果傳送或接收證書配置不正確或過期，通訊將失敗。

3. SEG需要驗證證書頒發機構清單中是否存在正確的目標中間證書和根證書。

4.從SEG cli進行簡單的Telnet測試，以驗證DNS文本記錄和對策略Web伺服器的基本響應測試。

- 從cli > dig _mta-sts.domain.com txt進行DNS查詢：

;;答案部分：
_mta-sts.domain.com。0（在TXT中）「v=STSv1;id=12345678598Z;"

- 通過Telnet從cli > telnet mta-sts.domain.com 443驗證基本的Web伺服器可訪問性：
- 使用常規Web瀏覽器檢視MTA-STS策略。
  - https://mta-sts.domain.com/.well-known/mta-sts.txt

```
version: STSv1
mode: enforce
mx: *.mail123.domain.com
max_age: 604800
```

相關資訊

- 思科安全電子郵件網關啟動頁面以支援指南

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。